EUROPA-
KOMMISSIONEN

DEN EUROPÆISKE UNIONS
HØJTSTÅENDE
REPRÆSENTANT
FOR UDENRIGSANLIGGENDER
OG SIKKERHEDSPOLITIK

Bruxelles, den 7.2.2013
JOIN(2013) 1 final

FÆLLES MEDDELELSE TIL EUROPA-PARLAMENTET, RÅDET, DET EUROPÆISKE ØKONOMISKE OG SOCIALE UDVALG OG REGIONSUDVALGET

EU-strategi for cybersikkerhed:

Et åbent, sikkert og beskyttet cyberspace

FÆLLES MEDDELELSE TIL EUROPA-PARLAMENTET, RÅDET, DET EUROPÆISKE ØKONOMISKE OG SOCIALE UDVALG OG REGIONSUDVALGET

EU-strategi for cybersikkerhed:

Et åbent, sikkert og beskyttet cyberspace

1. INDLEDNING

1.1. Baggrund

I de sidste tyve år har internettet og mere bredt cyberspace haft enorm indvirkning på alle samfundets sider. Vores hverdag, grundlæggende rettigheder, sociale relationer og økonomier er afhængige af, at informations- og kommunikationsteknologien fungerer gnidningsløst. Det åbne og frie cyberspace har fremmet den politiske og sociale integration i hele verden; det har nedbrudt barrierer mellem lande, samfund og borgere og således muliggjort samspil og udveksling af information og idéer i hele verden; det har skabt et forum for ytringsfriheden og udøvelsen af grundlæggende rettigheder og rustet mennesker i deres søgen efter demokratiske og mere lige samfund – mest iøjnefaldende under det arabiske forår.

For at cyberspace fortsat kan være åbent og frit, må de samme normer, principper og værdier, som EU opretholder offline, også gælde online. De grundlæggende rettigheder, demokratiet og retsstaten skal beskyttes i cyberspace. Vores frihed og velstand afhænger mere og mere af et solidt og innovativt internet, som vil fortsætte sin blomstrende udvikling, hvis det fremmes af innovationen i den private sektor og civilsamfundet. Men frihed online kræver også sikkerhed og beskyttelse. Cyberspace bør beskyttes mod hændelser, ondsindede handlinger og misbrug, og de offentlige myndigheder spiller en vigtig rolle i bestræbelserne på at sikre et frit og sikkert cyberspace. De offentlige myndigheder har flere opgaver: at sikre adgang og åbenhed, at respektere og beskytte de grundlæggende rettigheder online og at opretholde internettets pålidelighed og interoperabilitet. Men den private sektor ejer og driver store dele af cyberspace, og hvis et initiativ skal lykkes, er det derfor nødvendigt at dens ledende rolle anerkendes.

Informations- og kommunikationsteknologi er blevet rygraden i vores økonomiske vækst og er en afgørende ressource, som alle økonomiske sektorer baserer sig på. Den understøtter nu de komplekse systemer, som får vores økonomier til at fungere i nøglesektorer som f.eks. finanssektoren, sundhed, energi og transport, og mange forretningsmodeller bygger på konstant adgang til internettet og informationssystemernes gnidningsløse funktion.

Europa vil med fuldførelsen af det digitale indre marked kunne øge sit BNP med næsten 500 mia. EUR om året[1], svarende til gennemsnitligt 1 000 EUR pr. person. Hvis de nye indbyrdes forbundne teknologier, herunder e-betalinger, cloud computing og kommunikation mellem maskiner[2], virkelig skal tage afsæt, er det nødvendigt, at borgerne har tiltro og tillid. Desværre har en Eurobarometer-undersøgelse[3] i 2012 vist, at næsten en tredjedel af europæerne tvivler på deres evne til at bruge internettet til banktransaktioner eller køb. Et overvældende flertal har også sagt, at de undgår at afsløre personlige oplysninger online, fordi

[1] Http://www.epc.eu/DSM/2/study_by_copenhagen.pdf

[2] F.eks. planter med tilknyttede sensorer til at kommunikere med sprinkleranlægget, når det er tid til vanding.

[3] 2012 Special Eurobarometer 390 on Cybersecurity

de er bekymrede for sikkerheden. I hele EU har mere end én ud af ti internetbrugere allerede været udsat for internetbedrageri.

I de seneste år har man kunnet konstatere, at den digitale verden giver enorme fordele, men også, at den er sårbar. Cybersikkerhedshændelserne[4], som kan være tilsigtede eller utilsigtede, vokser med alarmerende hast og vil kunne afbryde forsyningen af væsentlige tjenester, som vi tager for givet, f.eks. vand, sundhed, elektricitet eller mobiltjenester. Truslerne kan have forskellig oprindelse — der kan bl.a. være tale om kriminelle angreb, politisk motiverede angreb, terrorangreb eller statsstøttede angreb samt naturkatastrofer og utilsigtede fejl.

EU's økonomi er allerede berørt af cyberkriminelle[5] aktiviteter, der er rettet mod den private sektor og enkeltpersoner. Cyberkriminelle anvender stadig mere sofistikerede metoder til at bryde ind i informationssystemer, stjæle kritiske data eller kræve løsepenge af virksomheder. Stigningen i økonomisk spionage og statsstøttede aktiviteter i cyberspace udgør en ny kategori af trusler mod offentlige myndigheder og virksomheder i EU.

I lande uden for EU kan offentlige myndigheder også misbruge cyberspace til overvågning og kontrol over deres egne borgere. EU kan imødegå denne situation ved at fremme frihed på nettet og sikre overholdelse af de grundlæggende rettigheder på nettet.

Alle disse faktorer ligger til grund for, at offentlige myndigheder i hele verden er gået i gang med at udvikle strategier for cybersikkerhed og behandle cyberspace som et stadig vigtigere internationalt anliggende. Tiden er inde til, at EU optrapper sin indsats på dette område. Dette forslag til en EU-strategi for cybersikkerhed, som er fremsat af Kommissionen og Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik (den højtstående repræsentant) skitserer EU's vision på dette område, præciserer de respektive roller og ansvarsområder og udstikker de påkrævede foranstaltninger på grundlag af en stærk og effektiv beskyttelse og fremme af borgernes rettigheder, med henblik på at gøre EU's online-miljø til det sikreste i verden.

1.2. Principper for cybersikkerhed

Det grænseløse internettet med dets mange niveauer er blevet et af de mest effektive instrumenter til at opnå globale fremskridt, uden tilsyn eller regulering fra det offentliges side. Den private sektor bør fortsat spille en ledende rolle i forbindelse med opbygningen og den daglige forvaltning af internettet, men der i stigende grad behov for krav om gennemsigtighed, ansvarlighed og sikkerhed. I denne strategi præciseres det, hvilke principper der bør ligge til grund for politikken for cybersikkerhed i EU og på internationalt plan.

---

[4] Ved cybersikkerhed forstås normalt de beskyttelsesforanstaltninger og tiltag, der kan iværksættes til at beskytte cyberspace på både civile og militære områder mod trusler, der er forbundet med eller kan skade dets indbyrdes afhængige net og informationsinfrastruktur. I forbindelse med cybersikkerhed tilstræbes det at bevare netværkenes og infrastrukturens tilgængelighed og integritet og beskytte fortroligheden af de oplysninger, de indeholder.

[5] Ved cyberkriminalitet forstås normalt en bred vifte af forskellige kriminelle aktiviteter, der omfatter computere og informationssystemer enten som primært værktøj eller som primært mål. Cyberkriminalitet omfatter traditionelle overtrædelser (f.eks. svig, forfalskning og identitetstyveri), indholdsrelaterede overtrædelser (f.eks. onlineudbud af børnepornografi eller tilskyndelse til racehad) og overtrædelser, der udelukkende er rettet mod computere og informationssystemer (f.eks. angreb på informationssystemer, denial of service og malware).

EU's centrale værdier gælder lige så meget i den digitale som i den fysiske verden

De love og normer, der gælder for andre områder af vores dagligdag, gælder også i forbindelse med cyberspace.

Beskyttelse af de grundlæggende rettigheder, ytringsfriheden, personoplysninger og privatlivets fred

Der kan kun opnås en fornuftig og effektiv cybersikkerhed, hvis denne sikkerhed baseres på de grundlæggende rettigheder og frihedsrettigheder, der er nedfældet i EU's charter om grundlæggende rettigheder, og EU's centrale værdier. Tilsvarende kan enkeltpersoners rettigheder ikke sikres uden sikre net og systemer. Enhver form for informationsudveksling i forbindelse med cybersikkerhed bør, når der er tale om personoplysninger, være i overensstemmelse med EU's databeskyttelseslovgivning og i fuldt omfang tage højde for enkeltpersoners rettigheder på dette område.

Adgang for alle

I betragtning af, hvor meget den digitale verden betyder for samfundsaktiviteterne, udgør begrænset eller ingen adgang til internettet og digital analfabetisme et handicap for borgerne. Alle bør have adgang til internettet og til en uhindret informationsstrøm. Internettets integritet og sikkerhed skal sikres for at muliggøre sikker adgang for alle.

Demokratisk og effektiv forvaltning med mange aktører

Den digitale verden kontrolleres ikke af en enkelt enhed. Der findes i øjeblikket mange interesseparter, bl.a. mange kommercielle og ikke-statslige enheder, der er involveret i den daglige ledelse af internetressourcer, -protokoller og -standarder og i den fremtidige udvikling af internettet. EU bekræfter på ny, at alle interesseparter i den nuværende forvaltningsmodel for internettet er vigtige, og støtter denne forvaltningstilgang med inddragelse af forskellige interesseparter[6].

Et fælles ansvar for sikkerhed

I og med at mennesker på alle områder af deres liv bliver mere og mere afhængige af informations- og kommunikationsteknologi, er der svagheder, som skal indkredses ordentligt, analyseres grundigt og afhjælpes eller mindskes. Alle relevante aktører - uanset om det er offentlige myndigheder, den private sektor eller enkelte borgere - er nødt til at erkende dette fælles ansvar, træffe foranstaltninger til at beskytte sig selv og om nødvendigt finde en koordineret løsning for at styrke cybersikkerheden.

2. STRATEGISKE PRIORITETER OG TILTAG

EU bør beskytte et online-miljø, der giver størst mulig frihed og sikkerhed til gavn for alle. Samtidig med at det anerkendes, at det først og fremmest er medlemsstaternes opgave at behandle sikkerhedsudfordringer i cyberspace, foreslås der i denne strategi specifikke tiltag, der kan styrke indsatsen i EU som helhed. Disse tiltag er både kort- og langsigtede og

[6] Se også KOM(2009) 277, meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om "Forvaltning af internettet: de næste skridt".

omfatter forskellige politikinstrumenter[7] og typer af aktører, både i EU-institutionerne, medlemsstaterne og industrien.

EU-visionen i denne strategi fokuserer på fem strategiske prioriteter, som behandler de udfordringer, der er anført ovenfor:

- Opnåelse af cyberrobusthed
- Drastisk mindskelse af cyberkriminalitet
- Udvikling af cyberforsvarspolitik og -kapacitet i forbindelse med den fælles sikkerheds- og forsvarspolitik (FSFP)
- Udvikling af de industrielle og teknologiske ressourcer til at fremme cybersikkerhed
- Fastlæggelse af en kohærent international cyberspacepolitik i EU og fremme af centrale EU-værdier.

2.1. Opnåelse af cyberrobusthed

For at fremme cyberrobustheden i EU skal både de offentlige myndigheder og den private sektor udvikle deres kapacitet og samarbejde effektivt. På baggrund af de positive resultater, der er opnået under hidtidige aktiviteter[8], vil yderligere EU-tiltag kunne bidrage til bl.a. at bekæmpe cyberkriminalitetsrisici og –trusler, der indebærer en grænseoverskridende dimension, og til at gennemføre en koordineret indsats i nødsituationer. Dette vil i høj grad støtte et velfungerende indre marked og øge den interne sikkerhed i EU.

Europa vil fortsat være sårbar, hvis der ikke gøres en betragtelig indsats for at styrke den offentlige og private sektors kapacitet, ressourcer og metoder til at forebygge, detektere og håndtere hændelser i forbindelse med cybersikkerhed. Det er grunden til, at Kommissionen har udarbejdet en strategi for net- og informationssikkerhed (NIS)[9]. **Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA)** blev oprettet i 2004[10], og Rådet og Parlamentet er i færd med at drøfte en ny forordning for at styrke ENISA og ajourføre dets mandat[11]. Desuden kræves det i rammedirektivet om elektronisk kommunikation[12], at udbydere af elektroniske kommunikationstjenester på passende vis skal styre risiciene for deres net og indberette væsentlige brud på sikkerheden. Desuden kræves det i EU's databeskyttelseslovgivning[13], at de registeransvarlige skal sikre databeskyttelseskrav og beskyttelsesforanstaltninger, herunder sikkerhedsrelaterede foranstaltninger, og at de i forbindelse med offentligt tilgængelige elektroniske kommunikationstjenester skal indberette hændelser, der indebærer brud på persondatasikkerheden, til de kompetente nationale myndigheder.

---

7 Tiltag i forbindelse med informationsudveksling bør, når der er tale om personoplysninger, være i overensstemmelse med EU's databeskyttelseslovgivning.

8 Se henvisningerne i denne meddelelse og i konsekvensanalysen i arbejdsdokumentet fra Kommissionens tjenestegrene, der ledsager Kommissionens forslag til et direktiv om net- og informationssikkerhed, navnlig afsnit 4.1.4, 5.2, bilag 2, bilag 6 og bilag 8.

9 I 2001 vedtog Kommissionen meddelelsen "Net- og informationssikkerhed: Forslag til en europæisk strategi" (KOM(2001) 298, endelig.); I 2006 vedtog Kommissionen en strategi for et sikkert informationssamfund (KOM(2006) 251). Siden 2009 har Kommissionen endvidere vedtaget en handlingsplan og en meddelelse om beskyttelse af kritisk informationsinfrastruktur (KOM(2009) 149, godkendt ved Rådets resolution 2009/C 321/01, og KOM(2011) 163, godkendt ved Rådets konklusioner 10299/11).

10 Forordning (EF) nr. 460/2004

11 KOM(2010) 521. De tiltag, der foreslås i denne strategi, medfører ikke ændringer af ENISA's nuværende eller fremtidige mandat.

12 Artikel 13a og 13b i direktiv 2002/21/EF.

13 Artikel 17 i direktiv 95/46/EF; artikel 4 i direktiv 2002/58/EF.

Trods fremskridt, som er baseret på frivillige forpligtelser, er der fortsat huller i hele EU, navnlig hvad angår national kapacitet, koordination i tilfælde af grænseoverskridende hændelser og den private sektors deltagelse og beredskab. Denne strategi ledsages af et forslag til **lovgivning**, der navnlig skal:

- fastsætte fælles mindstekrav til NIS på nationalt plan, der vil forpligte medlemsstaterne til at: udpege nationale NIS-kompetente myndigheder, oprette et velfungerende it-udrykningshold (CERT), og vedtage en national NIS-strategi og en national NIS-samarbejdsplan. Kapacitetsopbygning og koordination vedrører også EU-institutionerne: i 2012 blev der oprettet et fast it-udrykningshold, der er ansvarligt for sikkerheden i it-systemerne i EU's institutioner, agenturer og organer ("CERT-EU")
- fastlægge koordinerede forebyggelses-, detekterings-, afbødnings- og indsatsmekanismer, der muliggør informationsudveksling og gensidig bistand mellem de nationale NIS-kompetente myndigheder. De nationale NIS-kompetente myndigheder vil blive bedt om at sørge for et hensigtsmæssig EU-dækkende samarbejde, navnlig på grundlag af en EU-plan for NIS-samarbejde, der udformes med henblik på at håndtere cyberhændelser med en grænseoverskridende dimension. Dette samarbejde vil også bygge videre på de fremskridt, der er gjort i forbindelse med det europæiske forum for medlemsstaterne (EFMS)[14], der har haft produktive drøftelser og udvekslinger om en offentlig NIS-politik og kan integreres i samarbejdsmekanismen, når den er på plads
- forbedre den private sektors deltagelse og beredskab. Da størstedelen af nettene og informationssystemerne ejes og drives privat, er det afgørende at forbedre samarbejdet med den private sektor for at fremme cybersikkerheden. Den private sektor bør på det tekniske plan udvikle sin egen cyberrobusthed og udveksle den bedste praksis på tværs af de forskellige sektorer. De værktøjer, der er udviklet af industrien til at reagere på hændelser, påvise årsager og gennemføre kriminaltekniske undersøgelser, bør også gavne den offentlige sektor.

Men aktørerne i den private sektor mangler stadig effektive incitamenter til at give pålidelige data om forekomsten eller virkningen af NIS-hændelser, indføre en risikostyringskultur eller investere i sikkerhedsløsninger. Derfor tager den foreslåede lovgivning sigte på at sikre, at aktørerne på en række centrale områder (såsom energi, transport, bankvæsen, børser, katalysatorer af centrale internettjenester og offentlige myndigheder) vurderer de cybersikkerhedsrisici, de står over for, gennem passende risikostyring sørger for, at net og informationssystemer er pålidelige og robuste, og udveksler de pågældende oplysninger med de nationale NIS-kompetente myndigheder. Hvis der indføres en cybersikkerhedskultur, vil det kunne forbedre forretningsmulighederne og konkurrenceevnen i den private sektor, som vil kunne gøre cybersikkerhed til et salgsargument.

Disse enheder vil til de nationale NIS-kompetente myndigheder skulle indberette de hændelser, der i betydelig grad påvirker kontinuiteten i vigtige tjenesteydelser og leveringen af varer, som er afhængige af forskellige net og informationssystemer.

De nationale NIS-kompetente myndigheder bør samarbejde og udveksle information med andre tilsynsmyndigheder, navnlig myndigheder med ansvar for beskyttelse af personoplysninger. De NIS-kompetente myndigheder bør på deres side indberette hændelser af formodet alvorlig kriminel art til de retshåndhævende myndigheder. De nationale

[14] Det europæiske forum for medlemsstaterne blev iværksat via KOM(2009) 149 som en platform til at fremme drøftelser mellem medlemsstaternes offentlige myndigheder om gode strategier for kritiske informationsinfrastrukturers sikkerhed og robusthed.

kompetente myndigheder bør også på et særligt websted regelmæssigt offentliggøre uklassificerede informationer om igangværende tidlig varsling af hændelser og risici og om koordinerede indsatser. De retlige forpligtelser bør hverken erstatte eller forhindre, at der udvikles uformelt og frivilligt samarbejde, bl.a. mellem den offentlige og den private sektor, for at øge sikringsniveauerne og forbedre udvekslingen af oplysninger og bedste praksis. Navnlig er det europæiske offentlig-private partnerskab for en robust ikt-infrastruktur (EP3R[15]) en god og solid platform på EU-niveau, som bør udvikles yderligere.

Gennem Connecting Europe-faciliteten (CEF)[16] vil der kunne ydes økonomisk støtte til vigtig infrastruktur, som forbinder medlemsstaternes NIS-kapacitet, således at det gøres lettere at samarbejde i hele EU.

Endelig er det vigtigt, at der på EU-niveau gennemføres øvelser i cyberhændelser for at simulere samarbejdet mellem medlemsstaterne og den private sektor. Den første øvelse med inddragelse af medlemsstaterne blev gennemført i 2010 ("Cyber Europe 2010") og den anden, som også den private sektor deltog i, fandt sted i oktober 2012 ("Cyber Europe 2012"). I november 2011 blev der gennemført en skrivebordsøvelse for EU og USA ("Cyber Atlantic 2011"). Der er planlagt flere øvelser for de kommende år, bl.a. med internationale partnere.

Kommissionen vil:

- videreføre sine aktiviteter, der gennemføres af Det Fælles Forskningscenter, i tæt koordination med medlemsstaternes myndigheder og ejere og operatører af kritisk infrastruktur for at indkredse NIS-svaghederne i den europæiske kritiske infrastruktur og fremme udviklingen af robuste systemer.
- iværksætte et EU-finansieret pilotprojekt[17] i begyndelsen af 2013 om **bekæmpelse af botnet and malware** for at skabe en ramme for koordination og samarbejde mellem EU's medlemsstater, organisationer i den private sektor som f.eks. internettjenesteudbydere og internationale partnere.

Kommissionen anmoder ENISA om:

- at hjælpe medlemsstaterne med at udvikle en **stærk national cyberrobusthed**, især ved at opbygge ekspertise om sikkerhed og robusthed i industrielle styringssystemer og transport- og energiinfrastruktur
- i 2013 at undersøge, om det kan lade sig gøre at indføre Computer Security Incident Response Team(s) for industrielle styringssystemer (ICS-CSIRT) for EU.
- fortsat at støtte medlemsstaterne og EU-institutionerne i bestræbelserne for at gennemføre regelmæssige **fælleseuropæiske øvelser i cyberhændelser**, som også vil udgøre det operationelle grundlag for EU's deltagelse i internationale

[15] Det europæiske offentlig-private partnerskab for en robust infrastruktur blev iværksat via KOM(2009) 149. Denne platform indledte arbejdet og fremmede samarbejdet mellem den offentlige og den private sektor om identifikation af vigtige aktiver, ressourcer, funktioner og basiskrav for en robust infrastruktur samt samarbejdsbehov og mekanismer til at reagere på omfattende forstyrrelser med virkninger for elektronisk kommunikation.

[16] https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. CEF budgetpost 09.03.02 - Telenet (til at fremme sammenkobling og interoperabilitet mellem de nationale offentlige tjenester online samt adgangen til disse net).

[17] CIP-ICT PSP-2012-6, 325188. Det har et samlet budget på 15 mio. EUR, med en EU-finansiering på 7,7 mio. EUR.

cyberhændelsesøvelser.

Kommissionen opfordrer Europa-Parlamentet og Rådet til:

- hurtigt at vedtage forslaget til et direktiv om et **højt fælles niveau for net- og informationssikkerhed (NIS)** i hele EU, som tager fat om kapacitet og beredskab, samarbejde på EU-plan, indførelse af risikostyring og informationsudveksling om NIS.

Kommissionen anmoder industrien om:

- at føre an med at **investere** i et højt cybersikkerhedsniveau og i højere grad udveksle bedste praksis og information på sektorplan og med de offentlige myndigheder for at sikre en stærk og effektiv beskyttelse af aktiver og enkeltpersoner, navnlig gennem offentlig-private partnerskaber som f.eks. EP3R og Trust in Digital Life (TDL)[18].
-

Bevidstgørelse

Alle har ansvaret for at sørge for cybersikkerhed. Slutbrugerne spiller en afgørende rolle for sikkerheden i net og informationssystemer: de skal gøres opmærksomme på onlinerisici og rustes til at træffe enkle foranstaltninger til at beskytte sig mod dem.

I de seneste år er der udviklet adskillige initiativer, som bør videreføres. Navnlig har ENISA været involveret i oplysningskampagner ved at offentliggøre rapporter, tilrettelægge workshopper for eksperter og udvikle offentlig-private partnerskaber. Europol, Eurojust og de nationale databeskyttelsesmyndigheder arbejder også aktivt inden for oplysning. I oktober 2012 gennemførte ENISA sammen med visse medlemsstater den "europæiske cybersikkerhedsmåned". Oplysning er et af de områder, som EU's og USA's fælles arbejdsgruppe om cybersikkerhed og cyberkriminalitet[19] søger at fremme, og det er også afgørende i forbindelse med programmet for et sikrere internet[20] (fokuseret på børns sikkerhed online).

Kommissionen anmoder ENISA om:

- i 2013 at foreslå en køreplan for et "net- og informationssikkerhedskørekort" som et frivilligt certificeringsprogram til at fremme it-fagfolks færdigheder og kompetence (f.eks. administratorer af websteder).

Kommissionen vil:

- med støtte fra ENISA tilrettelægge en **cybersikkerhedskonkurrence** i 2014, hvor

[18] http://www.trustindigitallife.eu/

[19] Denne arbejdsgruppe, der blev nedsat i forbindelse med topmødet mellem EU og USA i november 2010 (MEMO/10/597), har til opgave at udvikle samarbejdstiltag vedrørende en lang række spørgsmål om cybersikkerhed og cyberkriminalitet.

[20] Programmet for et sikrere internet finansierer et netværk af ngo'er, der er aktive inden for børns velfærd online, et netværk af retshåndhævende organer, der udveksler oplysninger og bedste praksis vedrørende kriminel udnyttelse af internettet i forbindelse med udbredelse af materiale om seksuelt misbrug af børn, og et netværk af forskere, der indsamler oplysninger om onlineteknologiers anvendelse, risici og konsekvenser for børns liv.

universitetsstuderende vil konkurrere med forslag til NIS-løsninger.

Kommissionen opfordrer medlemsstaterne[21] til:

- fra og med 2013 at organisere en årlig **cybersikkerhedsmåned** med støtte fra ENISA og medinddragelse af den private sektor for at gøre slutbrugerne mere bevidste. Der vil også blive organiseret en samordnet cybersikkerhedsmåned mellem EU og USA, første gang i 2014.
- at **intensivere de nationale bestræbelser inden for NIS-uddannelse og -undervisning** ved at indføre: NIS-undervisning i skolerne i 2014; NIS-undervisning og udvikling af sikkert software og persondatabeskyttelse for datalogistuderende; og grundlæggende NIS-undervisning for ansatte i offentlige administrationer.

Kommissionen opfordrer industrien til:

- at fremme **bevidstgørelsen om cybersikkerhed på alle niveauer**, både i forretningspraksis og i kundekontakt. Industrien bør især gøre sig overvejelser om, hvordan man kan gøre administrerende direktører og bestyrelser mere ansvarlige for at sørge for cybersikkerhed.

2.2. Drastisk mindskelse af cyberkriminalitet

Jo mere vi bruger den digitale verden, jo flere muligheder får de cyberkriminelle. Cyberkriminalitet er en af de hurtigst voksende former for kriminalitet, idet der på verdensplan er mere end en million mennesker, som hver dag bliver ofre herfor. Cyberkriminalitet og cyberkriminelle net bliver mere og mere sofistikerede, og vi skal have de rette operationelle værktøjer og den rette kapacitet til at takle dem. Cyberkriminalitet er forbundet med høj profit og lav risiko, og de kriminelle udnytter ofte websteddomænernes anonymitet. Cyberkriminalitet kender ingen grænser – internettets globale udbredelse betyder, at de retshåndhævende myndigheder er nødt til at vedtage en koordineret og samarbejdsbaseret tilgang på tværs af grænserne for at kunne imødegå denne voksende trussel.

En stærk og effektiv lovgivning

EU og medlemsstaterne har brug for en stærk og effektiv lovgivning til at bekæmpe cyberkriminalitet. Europarådets konvention om it-kriminalitet, også kendt som Budapestkonventionen, er en bindende international traktat, som udgør en effektiv ramme for vedtagelsen af national lovgivning.

EU har allerede vedtaget lovgivning om cyberkriminalitet, herunder et direktiv om bekæmpelse af seksuel udnyttelse af børn og børnepornografi[22]. Man er i EU også ved at blive enige om et direktiv om angreb mod informationssystemer, især gennem brug af botnet.

---

[21] Også med inddragelse af relevante nationale myndigheder, herunder NIS-kompetente myndigheder og databeskyttelsesmyndigheder.

[22] Direktiv 2011/93/EU om erstatning af Rådets rammeafgørelse 2004/68/RIA.

Kommissionen vil:

- sikre, at direktiverne vedrørende cyberkriminalitet gennemføres og anvendes hurtigt
- indtrængende opfordre de medlemsstater, der endnu ikke har ratificeret **Europarådets Budapestkonvention om it-kriminalitet**, til at ratificere og gennemføre dens bestemmelser hurtigst muligt.

Styrkelse af den operationelle kapacitet til at bekæmpe cyberkriminalitet

Udviklingen af cyberkriminelle teknikker er i hastig stigning: de retshåndhævende myndigheder kan ikke bekæmpe cyberkriminalitet med forældede operationelle værktøjer. I øjeblikket har ikke alle EU-medlemsstater den operationelle kapacitet, de skal bruge til effektivt at imødegå cyberkriminalitet. Alle medlemsstater bør have effektive nationale enheder til bekæmpelse af cyberkriminalitet.

Kommissionen vil:

- gennem sine finansieringsprogrammer[23] bistå medlemsstaterne med at **identificere huller og styrke deres kapacitet** til at undersøge og bekæmpe cyberkriminalitet. Kommissionen vil endvidere støtte organer, der forbinder forskersamfundet/akademiske kredse, retshåndhævere og den private sektor, svarende til det arbejde, der i øjeblikket udføres af de af Kommissionen finansierede ekspertisecentre for cyberkriminalitet, som visse medlemsstater allerede har oprettet.
- sammen med medlemsstaterne koordinere indsatsen for at identificere den bedste praksis og de bedste tilgængelige teknikker, bl.a. med støtte fra JRC, for at bekæmpe cyberkriminalitet (f.eks. med hensyn til udvikling og brug af kriminaltekniske redskaber eller til trusselsanalyser).
- arbejde tæt sammen med det nye **europæiske center for bekæmpelse af cyberkriminalitet (EC3) under Europol og med Eurojust** for at afpasse sådanne initiativer med den bedste praksis på det operationelle plan.

Bedre koordination på EU-plan

EU kan supplere medlemsstaternes indsats ved at lette en koordineret og samarbejdsbaseret strategi, der samler retshåndhævende og retlige myndigheder og offentlige og private berørte parter både i og uden for EU.

Kommissionen vil:

- støtte det nye **europæiske center for bekæmpelse af cyberkriminalitet** (EC3) som europæisk kontaktpunkt i forbindelse med bekæmpelsen af cyberkriminalitet. Centret skal bistå med analyser og efterretning, støtte undersøgelser, sørge for

[23] For 2013, under programmet om forebyggelse og bekæmpelse af kriminalitet (ISEC). Efter 2013, under Fonden for Intern Sikkerhed (nyt instrument under FFR).

kriminaltekniske undersøgelser af høj kvalitet, fremme samarbejde, skabe kanaler for informationsudveksling mellem de kompetente myndigheder i medlemsstaterne, den private sektor og andre interesseparter og gradvis tjene som talerør for de retshåndhævende myndigheder[24].

- støtte indsatsen for at øge det ansvar, der påhviler registratorer af domænenavne, og sikre, at oplysningerne om websteders ejerskab er nøjagtige, på grundlag af håndhævelseshenstillingerne til ICANN (Internet Corporation for Assigned Names and Numbers), i overensstemmelse med EU-retten, herunder databeskyttelsesreglerne.
- på basis af den seneste lovgivning fortsat styrke EU's indsats for at bekæmpe seksuelt misbrug af børn online. Kommissionen har vedtaget en europæisk strategi for et bedre internet for børn[25] og har sammen med en række EU-lande og lande uden for EU lanceret en **global alliance mod seksuelt misbrug af børn online**[26]. Alliancen skal fremme yderligere tiltag fra medlemsstaternes side med støtte fra Kommissionen og EC3.

Kommissionen anmoder Europol (EC3) om:

- først at fokusere sin analytiske og operationelle støtte på medlemsstaternes undersøgelser af cyberkriminalitet for at hjælpe dem med at optrævle og forhindre kriminelle cybernet, primært i forbindelse med seksuelt misbrug af børn, betalingssvindel, botnet og uautoriseret adgang.
- regelmæssigt at udarbejde strategiske og operationelle rapporter om tendenser og nye trusler for at identificere prioriteter og fokusere på undersøgelsestiltag, der iværksættes af de hold, der skal bekæmpe cyberkriminalitet i medlemsstaterne.

Kommissionen anmoder Det Europæiske Politiakademi (Cepol) om i samarbejde med Europol:

- at koordinere udformningen og planlægningen af kurser med henblik på at udstyre retshåndhævelsesmyndighederne med den viden og ekspertise, der er nødvendig for effektivt at bekæmpe cyberkriminalitet.

Kommissionen anmoder Eurojust om:

- at identificere de væsentligste hindringer for det retlige samarbejde om undersøgelser vedrørende cyberkriminalitet og for koordinationen mellem medlemsstaterne og med tredjelande og at støtte undersøgelser og retsforfølgelse af cyberkriminalitet, på både operationelt og strategisk plan, samt uddannelse på området.

Kommissionen anmoder Eurojust og Europol (EC3) om:

- at gennemføre et tæt samarbejde, bl.a. via udveksling af information, for at effektivisere deres indsats for at bekæmpe cyberkriminalitet, i overensstemmelse med deres respektive mandater og kompetencer.

---

[24] Den 28. marts 2012 vedtog Europa-Kommissionen meddelelsen "Bekæmpelse af kriminalitet for digitale tidsalder - Oprettelse af et europæisk center til bekæmpelse af it-kriminalitet".

[25] KOM(2012) 196 endelig.

[26] Rådets konklusioner om en global alliance mod seksuelt misbrug af børn online (EU's og USA's fælles erklæring) af 7. og 8. juni 2012 og erklæringen om iværksættelsen af den globale alliance mod seksuelt misbrug af børn online (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm).

2.3. Udvikling af cyberforsvarspolitik og -kapacitet i forbindelse med rammerne for den fælles sikkerheds- og forsvarspolitik (FSFP)

Cybersikkerhedsindsatsen i EU omfatter også cyberforsvarsdimensionen. For bedre at ruste kommunikations- og informationssystemerne, der understøtter medlemsstaternes forsvars- og sikkerhedsinteresser, bør udbygningen af cyberforsvarskapaciteten koncentreres om detektering, indsats og genopretning i tilfælde af avancerede cybertrusler.

Da disse trusler er komplekse, bør der skabes større synergi mellem de civile og militære tilgange til at beskytte kritisk infrastruktur. Disse bestræbelser bør støttes af forskning og udvikling og tættere samarbejde mellem de offentlige myndigheder, den private sektor og den akademiske verden i EU. For at undgå overlapning vil EU undersøge mulighederne for, hvordan EU og NATO kan supplere deres bestræbelser for at gøre den kritiske infrastruktur, som medlemmerne af de to organisationer er afhængige af, i staten, forsvaret og på andre områder mere robust.

Den høje repræsentant vil fokusere på følgende hovedaktiviteter og opfordrer medlemsstaterne og Det Europæiske Forsvarsagentur til at samarbejde med henblik herpå:

- Vurdering af EU's operationelle cyberforsvarskrav og fremme af udviklingen af EU's cyberforsvarskapacitet og -teknologi for at håndtere alle aspekter af kapacitetsudvikling – herunder doktrin, ledelse, organisation, personale, uddannelse, teknologi, infrastruktur, logistik og interoperabilitet.

- Udvikling af EU's cyberforsvarspolitiske ramme til at beskytte net i forbindelse med FSFP-missioner og -operationer, herunder dynamisk risikostyring, bedre trusselsanalyse og informationsudveksling. Forbedring af mulighederne for cyberforsvarsundervisning og -øvelser for militæret i europæisk og multinational kontekst, herunder integration af cyberforsvarselementer i de eksisterende programmer.

- Fremme af dialogen og koordinationen mellem civile og militære aktører i EU – med særlig vægt på udveksling af god praksis, udveksling af oplysninger og hurtig varsling, håndtering af hændelser, risikovurdering, bevidstgørelse og prioritering af cybersikkerhed.

- Dialog med internationale partnere, herunder NATO, andre internationale organisationer og multinationale ekspertisecentre, for at sikre effektiv forsvarskapacitet, identificere samarbejdsområder og undgå overlapninger.

2.4. Udvikling af industrielle og teknologiske ressourcer til at fremme cybersikkerhed

Europa har en fremragende forsknings- og udviklingskapacitet, men mange af de globale førende udbydere af innovative ikt-produkter og -tjenesteydelser befinder sig uden for EU. Der er en risiko for, at Europa bliver for afhængig ikke kun af ikt, der produceres andre steder, men også af sikkerhedsløsninger, som udvikles uden for dets grænser. Det er vigtigt at sikre, at hardware- og softwarekomponenter, der produceres i EU og i tredjelande og anvendes i kritiske tjenester og infrastruktur samt også i stigende grad i mobile enheder, er pålidelige og sikre og garanterer, at personoplysninger beskyttes.

Fremme af et indre marked for cybersikkerhedsprodukter

Der kan kun opnås en høj grad af sikkerhed, hvis alle i værdikæden (f.eks. fabrikanter af materiel, udviklere af software og udbydere af informationssamfundstjenester) gør sikkerhed til en prioritet. Det ser dog ud til[27], at mange aktører stadig betragter sikkerhed som næsten endnu byrde, og der er begrænset efterspørgsel efter sikkerhedsløsninger. Det er nødvendigt, at der overholdes passende krav for cybersikkerhed i hele værdikæden for de ikt-produkter, der bruges i Europa. Den private sektor skal have incitamenter til at sørge for et højt niveau af cybersikkerhed - f.eks. vil mærker, der attesterer passende cybersikkerhed, kunne give virksomheder, der har gode præstationer og resultater inden for cybersikkerhed, et salgsargument og dermed også en konkurrencefordel. Desuden vil de forpligtelser, der er fastlagt i forslaget til NIS-direktiv, i betydelig grad kunne bidrage til at øge virksomhedernes konkurrenceevne i de omfattede sektorer.

Man bør også søge at fremme en fælleseuropæisk markedsefterspørgsel efter yderst sikre produkter. For det første tager denne strategi sigte på at øge samarbejdet og gennemsigtigheden for ikt-produkters sikkerhed. Der opfordres til, at der etableres en platform, der samler relevante europæiske offentlige og private interesseparter, for at fastlægge god cybersikkerhedspraksis for hele værdikæden og skabe gunstige markedsvilkår for udviklingen og indførelsen af sikre ikt-løsninger. Der bør primært fokuseres på nye incitamenter til at foretage en passende risikostyring og vedtage sikkerhedsstandarder og -løsninger og på mulighederne for at indføre frivillige EU-certificeringsordninger, der bygger på eksisterende ordninger i EU og på internationalt plan. Kommissionen vil arbejde for, at der vedtages en kohærent tilgang blandt medlemsstaterne for at undgå forskelle, der forårsager stedrelaterede ulemper for virksomheder.

For det andet vil Kommissionen støtte udviklingen af sikkerhedsstandarder og EU-dækkende frivillige certificeringsordninger inden for cloud computing, samtidig med at der tages behørigt hensyn til behovet for at sikre databeskyttelsen. Arbejdet bør koncentreres om sikkerhed i forsyningskæden, navnlig i kritiske økonomiske sektorer (industrielle styringssystemer, energi og transportinfrastruktur). Dette arbejde bør bygge på det løbende standardiseringsarbejde i de europæiske standardiseringsorganer (CEN, CENELEC og ETSI)[28], arbejdet i koordinationsgruppen for cybersikkerhed samt ekspertise fra ENISA, Kommissionen og andre relevante aktører.

Kommissionen vil:

- i 2013 lancere en offentlig-privat **platform for NIS-løsninger** til at udvikle incitamenter for indførelsen af sikre ikt-løsninger og god cybersikkerhed, som skal anvendes for ikt-produkter, der bruges i Europa.
- i 2014 foreslå anbefalinger til at sørge for cybersikkerheden for ikt i hele værdikæden på grundlag af denne platforms arbejde
- undersøge, hvordan større udbydere af ikt-hardware og -software vil kunne informere de nationale kompetente myndigheder om konstaterede sårbarheder, som vil kunne få betydelige sikkerhedsfølger.

[27] Se konsekvensanalysen i arbejdsdokumentet fra Kommissionens tjenestegrene, der ledsager Kommissionens forslag til et direktiv om net- og informationssikkerhed, pkt. 4.1.5.2.

[28] Navnlig inden for rammerne af standard M/490 for intelligente net for det første sæt standarder for intelligent net- og referencearkitektur.

Kommissionen anmoder ENISA om:

- i samarbejde med relevante nationale kompetente myndigheder, relevante interesseparter, internationale og europæiske standardiseringsorganer og Europa-Kommissionens fælles forskningscenter at udarbejde **tekniske retningslinjer og henstillinger til indførelsen af NIS-standarder og god NIS-praksis** i den offentlige og private sektor.

Kommissionen opfordrer offentlige og private interesseparter til:

- at fremme udvikling og indførelse af industristyrede **sikkerhedsstandarder**, tekniske standarder og principperne om indbygget sikkerhed og privatlivsbeskyttelse for fabrikanter af ikt-produkter og udbydere af ikt-tjenester, herunder cloud-udbydere. De nye generationer af software og hardware bør udstyres med **stærkere, integrerede og brugervenlige sikkerhedselementer**.
- at udarbejde industristyrede standarder for virksomhedernes præstationer inden for cybersikkerhed og forbedre de tilgængelige oplysninger til offentligheden ved at udvikle **sikkerhedsmærkning** eller kvalitetsmærker, der hjælper forbrugerne med at finde rundt på markedet.

Fremme af F&U-investeringer

F&U kan bidrage til en stærk industripolitik, fremme en pålidelig europæisk ikt-industri, sætte skub i det indre marked og reducere Europas afhængighed af udenlandsk teknologi. F&U bør udfylde de teknologiske huller inden for ikt-sikkerhed, forberede den næste generation af sikkerhedsudfordringer, tage hensyn til den konstante udvikling i brugernes behov og udnytte teknologier med dobbelt anvendelse. Den bør også fortsat støtte udviklingen af kryptografi. Dette skal suppleres med en indsats for at omsætte F&U-resultater til kommercielle løsninger ved at tilvejebringe de nødvendige incitamenter og hensigtsmæssige politiske betingelser.

EU bør gøre bedst mulig brug af Horisont 2020[29]-rammeprogrammet for forskning og innovation, der skal lanceres i 2014. Kommissionens forslag indeholder specifikke mål for pålidelig ikt og bekæmpelse af cyberkriminalitet, som er i tråd med denne strategi. Horisont 2020 vil støtte sikkerhedsrelateret forskning i forbindelse med nye ikt-teknologier, tilvejebringe løsninger for at opnå "end-to-end"-sikre ikt-systemer, -tjenester og -applikationer, tilvejebringe incitamenter til at indføre og gennemføre eksisterende løsninger og tage fat om spørgsmål om interoperabilitet mellem net og informationssystemer. På EU-plan vil der især blive udvist opmærksomhed om at optimere og bedre koordinere forskellige finansieringsprogrammer (Horisont 2020, Fonden for Intern Sikkerhed, EDA-forskning, inklusive det europæiske rammesamarbejde).

[29] Horisont 2020 er det finansielle instrument til at gennemføre Innovation i EU, som er et Europa 2020-flagskibsinitiativ, der har til formål at sikre Europas globale konkurrenceevne. Fra 2014 til 2020 vil EU's nye rammeprogram for forskning og innovation indgå i indsatsen for at skabe ny vækst og nye arbejdspladser i Europa.

Kommissionen vil:

- anvende Horisont 2020 til at tage fat om forskellige aspekter af ikt-fortrolighed og –sikkerhed, fra F&U til innovation og anvendelse. Under Horisont 2020 vil der også blive udviklet redskaber og instrumenter til at bekæmpe kriminelle og terroristiske aktiviteter, der er rettet mod cyberspace.
- etablere mekanismer til bedre at koordinere EU-institutionernes og medlemsstaternes forskningsdagsordener og tilskynde medlemsstaterne til at investere mere i F&U.

Kommissionen opfordrer indtrængende medlemsstaterne til:

- inden udgangen af 2013 at udvikle god praksis for anvendelsen af **de offentlige myndigheders købekraft** (f.eks. via offentlige indkøb) til at stimulere udviklingen og anvendelsen af sikkerhedselementer ved ikt-produkter og -tjenester.
- at fremme tidlig inddragelse af industrien og den akademiske verden i udviklingen og koordinationen af løsninger. Dette bør ske ved at man bedst muligt udnytter Europas industribase og dertil knyttet teknologisk innovation inden for F&U, og tiltagene bør koordineres mellem de civile og militære organisationers forskningsprogrammer.

Kommissionen anmoder Europol og ENISA om:

- at identificere nye tendenser og behov i betragtning af udviklingen i cyberkriminalitet og mønstrene for cybersikkerhed, således at der kan udarbejdes digitale kriminaltekniske værktøjer og teknologier, som er hensigtsmæssige.

Kommissionen opfordrer offentlige og private interesseparter til:

- i samarbejde med forsikringsbranchen at udvikle **harmoniseret metrik til beregning af risikopræmier**, som ville give virksomheder, der har foretaget investeringer i sikkerhed, mulighed for at nyde fordel af et lavere risikopræmier.

2.5. Fastlæggelse af en kohærent international cyberspacepolitik i EU og fremme af EU's centrale værdier

At bevare et åbent, frit og sikkert cyberspace er en global udfordring, som EU bør løse sammen med de relevante internationale partnere og organisationer, den private sektor og civilsamfundet.

EU vil i sin internationale cyberspacepolitik søge at fremme internettets åbenhed og frihed, anspore bestræbelserne for at udvikle adfærdsregler og anvende eksisterende internationale love i cyberspace. EU vil også arbejde for at bygge bro over den digitale kløft og vil deltage aktivt i de internationale bestræbelser på at opbygge cybersikkerhedskapacitet. EU's internationale engagement i cyberspørgsmål vil være styret af EU's centrale værdier: menneskets værdighed, frihed, demokrati, lighed, retsstatsprincippet og respekten for de grundlæggende rettigheder.

Integrering af cyberspacespørgsmål i EU's eksterne forbindelser og fælles udenrigs- og sikkerhedspolitik

Kommissionen, den højtstående repræsentant og medlemsstaterne bør udarbejde en kohærent international EU-politik for cyberspace, som sigter mod større samarbejde og stærkere forbindelser med centrale internationale partnere og organisationer og med civilsamfundet og den private sektor. EU's samråd med internationale partnere om cyberspørgsmål bør udformes, koordineres og gennemføres således, at der tilføres merværdi til de eksisterende bilaterale dialoger mellem EU's medlemsstater og tredjelande. EU vil lægge fornyet vægt på dialog med tredjelande, med særligt fokus på ligesindede partnere, som deler EU's værdier. Det vil arbejde for at opnå et højt niveau af databeskyttelse, bl.a. for overførsel af personoplysninger til tredjelande. Med henblik på at løse de globale udfordringer i cyberspace vil EU søge tættere samarbejde med organisationer, der er aktive på dette område, såsom Europarådet, OECD, FN, OSCE, NATO, AU, ASEAN og OAS. På det bilaterale plan er samarbejdet med USA særligt vigtigt og vil blive udviklet yderligere, navnlig inden for rammerne af EU's og USA's fælles arbejdsgruppe om cybersikkerhed og cyberkriminalitet.

Et af de væsentligste elementer i EU's internationale cyberpolitik vil bestå i at fremme cyberspace som et område med frihed og grundlæggende rettigheder. En udvidet adgang til internettet bør fremme demokratiske reformer og demokrati i hele verden. En forøgelse af den globale konnektivitet bør ikke ledsages af censur eller af overvågning af masserne. EU bør anspore virksomhedernes sociale ansvar[30] og iværksætte internationale initiativer for at forbedre den globale koordination på dette område.

Ansvaret for et mere sikkert cyberspace ligger hos alle aktører i det globale informationssamfund, fra de enkelte borgere til staten. EU støtter bestræbelserne på at fastsætte normer for adfærd i cyberspace, som alle parter bør overholde. På samme måde som det i EU forventes, at borgerne respekterer deres samfundsmæssige pligter og ansvar og lovgivningen online, bør også staterne overholde normerne og den eksisterende lovgivning. For så vidt angår spørgsmål om international sikkerhed, ansporer EU udviklingen af tillidsskabende foranstaltninger med hensyn til cybersikkerhed for at øge gennemsigtigheden og mindske risikoen for misforståelser med hensyn til statens adfærd.

EU anbefaler ikke, at der skabes nye internationale retlige instrumenter for cyberanliggender.

De juridiske forpligtelser, der er nedfældet i den internationale konvention om borgerlige og politiske rettigheder, den europæiske menneskerettighedskonvention og EU's charter om grundlæggende rettigheder, bør også overholdes online. EU vil fokusere på, hvordan man sikrer, at disse foranstaltninger også håndhæves i cyberspace.

I forbindelse med bekæmpelsen af cyberkriminalitet er Budapestkonventionen et instrument, der kan ratificeres af tredjelande. Den kan bruges som model for udarbejdelsen af national lovgivning mod cyberkriminalitet og som grundlag for det internationale samarbejde på dette område.

Hvis der opstår væbnede konflikter, som omfatter cyberspace, vil den internationale humanitære ret og, hvis det er hensigtsmæssigt, menneskerettighedslovgivningen gælde i påkommende tilfælde. **Kapacitetsopbygning vedrørende cybersikkerhed og robust informationsinfrastruktur i tredjelande**

Den underliggende infrastruktur, der leverer og letter kommunikationstjenester, vil kunne fungere mere gnidningsløst, hvis det internationale samarbejde styrkes. Dette omfatter udveksling af bedste praksis, udveksling af oplysninger, øvelser i tidlig varsling og fælles

[30] En ny EU-strategi 2011-2014 for virksomhedernes sociale ansvar, KOM(2011) 681 endelig.

styring af hændelser osv. EU vil bidrage til dette mål ved at intensivere de igangværende internationale bestræbelser på at styrke de samarbejdsnet for beskyttelse af kritisk informationsinfrastruktur, som de offentlige myndigheder og den private sektor deltager i.

Det er ikke alle steder i verden, at man får udbytte af internettets positive virkninger, da man nogle steder ikke har en tilstrækkelig åben, sikker, interoperabel og pålidelig adgang. Den Europæiske Union vil derfor fortsat støtte landenes bestræbelser for at give deres befolkninger bedre adgang til internettet og forbedre brugen med henblik på at sikre dets integritet og sikkerhed og effektivt bekæmpe cyberkriminalitet.

I samarbejde med medlemsstaterne vil Kommissionen og den højtstående repræsentant:

- søge at udarbejde en kohærent international EU-politik for cyberspace for at øge samarbejdet med vigtige internationale partnere og organisationer, integrere cyberspørgsmål i FUSP og forbedre koordinationen af globale cyberanliggender
- støtte udviklingen af adfærdsnormer og tillidsskabende foranstaltninger inden for cybersikkerhed; fremme dialoger om, hvordan man anvender gældende folkeret i cyberspace og fremme Budapestkonventionen med henblik på bekæmpelse af cyberkriminalitet;
- medvirke til at fremme og beskytte grundlæggende rettigheder, herunder adgang til information og ytringsfrihed, med fokus på: a) udvikling af nye offentlige retningslinjer om ytringsfrihed online og offline; b) kontrol med eksport af produkter eller tjenester, der kan anvendes til censur eller masseovervågning online; c) udvikling af foranstaltninger og værktøjer til at udvide adgangen til internettet og gøre det mere åbent og robust med sigte på at bekæmpe censur eller masseovervågning inden for kommunikationsteknologi; d) ruste de berørte parter til at bruge kommunikationsteknologien til at fremme de grundlæggende rettigheder.
- samarbejde med internationale partnere og organisationer, den private sektor og civilsamfundet for at støtte den globale kapacitetsopbygning i tredjelande til at forbedre adgangen til information og til et åbent internet for at forhindre og imødegå cybertrusler, herunder uheld, cyberkriminalitet og cyberterrorisme, og for at styrke donorkoordinationen i forbindelse med styringen af opbygningen af kapacitet.
- anvende forskellige EU-støtteinstrumenter til kapacitetsopbygning i forbindelse med cybersikkerhed, herunder støtte til uddannelse af retshåndhævende, retligt og tekniske personale til at imødegå cybertrusler, samt støtte udarbejdelsen af relevante nationale politikker, strategier og institutioner i tredjelande.
- øge den politiske koordination og informationsdeling via de internationale netværker for beskyttelse af kritisk informationsinfrastruktur som f.eks. Meridian-netværket, samarbejde mellem NIS-kompetente myndigheder og andre parter.

3. ROLLER OG ANSVARSOMRÅDER

Cyberhændelser standser ikke ved grænserne i vores sammenkoblede digitale økonomi og samfund. Alle aktører, det være sig NIS-kompetente myndigheder, CERT, håndhævelsesmyndigheder eller industrien, må påtage sig et ansvar, både nationalt og på EU-plan, og samarbejde for at styrke cybersikkerheden. Da der kan være forskellige retlige rammer og retssystemer, som er involveret, er en af de vigtigste udfordringer for EU nu at præcisere, hvilke roller og ansvarsområder de mange involverede aktører har.

I betragtning af spørgsmålets kompleksitet og de mange forskellige aktører er løsningen ikke en centraliseret europæisk overvågning. De nationale regeringer er bedst placeret til at organisere forebyggelse og reaktion på cyberhændelser og -angreb og til at etablere kontakter og netværk med den private sektor og offentligheden på tværs af deres politikker og retlige rammer. Da risiciene potentielt eller rent faktisk er grænseoverskridende, vil en effektiv national indsats samtidig ofte kræve samarbejde på EU-plan. For at behandle spørgsmålet om cybersikkerhed på en omfattende måde bør aktiviteterne spænde over tre centrale piller - NIS, retshåndhævelse og forsvar – som også opererer inden for forskellige juridiske rammer:

3.1. Koordination mellem NIS-kompetente myndigheder/CERT, retshåndhævelsesmyndigheder og forsvar

På nationalt plan

Medlemsstaterne bør enten allerede nu eller som følge af denne strategi have strukturer til at håndtere cyberrobusthed, cyberkriminalitet og forsvar og bør opnå det kapacitetsniveau, der er nødvendigt for at håndtere cyberhændelser. Men da en række enheder kan have operationelt ansvar over forskellige dimensioner af cybersikkerhed, og da det er vigtigt at inddrage den private sektor, bør koordinationen på nationalt niveau optimeres på tværs af ministerierne. Medlemsstaterne bør i deres nationale strategier for cybersikkerhed fastlægge rollerne og ansvarsområderne for deres forskellige nationale enheder.

Der bør tilskyndes til udveksling af information mellem de nationale enheder og med den private sektor, så medlemsstaterne og den private sektor løbende kan danne sig et samlet billede af de forskellige trusler og bedre forstå nye tendenser og teknikker, der anvendes både til at udføre cyberangreb og til at reagere på dem hurtigere. Ved etableringen af nationale NIS-samarbejdsplaner, som aktiveres i tilfælde af cyberhændelser, bør medlemsstaterne kunne foretage en klar fordeling af roller og ansvarsområder og optimere reaktionsindsatsen.

På EU-plan

Ligesom på nationalt plan er der på EU-plan en række aktører, der beskæftiger sig med cybersikkerhed. Navnlig er ENISA, Europol/EC3 og EDA er tre agenturer, der beskæftiger sig med henholdsvis NIS, retshåndhævelse og forsvar. Disse agenturer har bestyrelser, hvor medlemsstaterne er repræsenteret, og tilbyder platforme for koordination på EU-plan.

Det vil blive tilstræbt at fremme koordinationen og samarbejdet mellem ENISA, Europol/EC3 og EDA på en række områder, hvor de alle er involveret, især med hensyn til tendensanalyse, risikovurdering, uddannelse og udveksling af eksempler på bedste praksis. De bør samarbejde, men samtidig bevare deres særlige karakteristika. Disse agenturer bør sammen med CERT-EU, Kommissionen og medlemsstaterne støtte oprettelsen af en anset gruppe tekniske og politiske eksperter på dette område.

Uformelle kanaler for koordination og samarbejde vil blive suppleret af mere strukturerede forbindelser. EU's militærstab og EDA's projektgruppe for cyberforsvar kan bidrage til at fremme koordinationen på forsvarsområdet. Programrådet for Europol/EC3 vil samle repræsentanter fra bl.a. Eurojust, Cepol, medlemsstaterne[31], ENISA og Kommissionen, som derigennem vil få mulighed for at udveksle særlig knowhow og sikre, at EC3's tiltag gennemføres i partnerskab, hvor alle berørte parters yderligere ekspertise anerkendes og deres mandat respekteres. ENISA's nye mandat skulle gøre det muligt at styrke forbindelserne med Europol og med de berørte parter i industrien. Det vigtigste er dog, at Kommissionens lovgivningsforslag om NIS vil fastlægge en ramme for samarbejdet via et netværk af nationale NIS-kompetente myndigheder og behandle spørgsmål om informationsudveksling mellem NIS-myndigheder og retshåndhævende myndigheder.

På internationalt plan

Kommissionen og den højtstående repræsentant sikrer sammen med medlemsstaterne en koordineret international indsats med hensyn til cybersikkerhed. Kommissionen og den høje repræsentant vil dermed forsvare EU's centrale værdier og fremme en fredelig, åben og gennemsigtig anvendelse af cyberteknologier. Kommissionen, den højtstående repræsentant og medlemsstaterne fører en politisk dialog med internationale partnere og internationale organisationer som f.eks. Europarådet, OECD, OSCE, NATO og FN.

3.2. EU-støtte i tilfælde af et større cyberhændelser eller -angreb

Større cyberhændelser eller -angreb kan få følger for EU's offentlige myndigheder, erhvervslivet og enkeltpersoner. Som følge af denne strategi, og især det foreslåede direktiv om net- og informationssikkerhed, bør forebyggelsen, detekteringen og imødegåelsen af cyberhændelser blive forbedret, og medlemsstaterne og Kommissionen bør holde hinanden bedre orienteret om større cyberhændelser eller -angreb. Indsatsmekanismerne vil dog være forskellige, alt efter hændelsens art, omfang og grænseoverskridende virkninger.

Hvis hændelsen har alvorlige konsekvenser for drifts/forretningskontinuiteten, foreslås det i NIS-direktivet, at der udløses nationale eller EU-dækkende NIS-samarbejdsplaner, afhængigt af hændelsens grænseoverskridende karakter. Netværket af NIS-kompetente myndigheder vil i den forbindelse blive anvendt til at udveksle information og støtte. Dette vil gøre det muligt at bevare og/eller genoprette de berørte net og tjenester.

Hvis hændelsen synes at vedrøre en kriminel handling, bør Europol/EC3 underrettes, således at de – sammen med de retshåndhævende myndigheder i de berørte lande – kan iværksætte en undersøgelse, bevare bevismateriale, identificere gerningsmændene og i sidste ende sikre, at disse retsforfølges.

Hvis hændelsen synes at vedrøre cyberspionage eller et statsstøttet angreb eller har følger for den nationale sikkerhed, vil de nationale sikkerheds- og forsvarsmyndigheder advare deres relevante kolleger, så de ved, at de er under angreb og kan forsvare sig. Derefter aktiveres mekanismerne for tidlig varsling, og, hvis det er påkrævet, krisestyring eller andre procedurer. En cyberhændelse eller et cyberangreb, der er særligt alvorlige, vil kunne udgøre tilstrækkelig begrundelse for, at en medlemsstat kan påberåbe sig EU's solidaritetsbestemmelse (artikel 222 i traktaten om Den Europæiske Unions funktionsmåde).

[31] Via repræsentation i EU's taskforce vedrørende cyberkriminalitet, der består af lederne for medlemsstaternes enheder for EU-cyberkriminalitet.

Hvis hændelsen synes at have kompromitteret personoplysninger, bør de nationale databeskyttelsesmyndigheder eller den nationale tilsynsmyndighed i henhold til direktiv 2002/58/EF inddrages.

Endelig vil man til håndteringen af cyberhændelser og -angreb kunne trække på kontaktnet og støtte fra internationale partnere. Dette kan omfatte teknisk afbødning, kriminalundersøgelse eller aktivering af krisestyrings- og indsatsmekanismer.

4. KONKLUSION OG OPFØLGNING

Dette forslag til en EU-strategi for cybersikkerhed, som er fremsat af Kommissionen og Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik, skitserer EU's vision og de tiltag, der kræves, på grundlag af en stærk beskyttelse og fremme af borgernes rettigheder, for at gøre EU's onlinemiljø til det sikreste i verden[32].

Denne vision kan kun virkeliggøres gennem et reelt partnerskab mellem mange aktører, hvor man påtager sig et ansvar og tager fat om de fremtidige udfordringer.

Kommissionen og den høje repræsentant opfordrer derfor Rådet og Europa-Parlamentet til, at de godkender strategien og bidrager til at realisere de skitserede tiltag. Der er også brug for stærk opbakning og engagement fra den private sektor og civilsamfundet, som er nøgleaktører, med henblik på at øge vores sikkerhedsniveau og beskytte borgernes rettigheder.

Det er nu, der skal handles. Kommissionen og den højtstående repræsentant er fast besluttet på at arbejde sammen med alle aktører til at opnå den sikkerhed, Europa har brug for. For at sikre at strategien gennemføres hurtigt og i lyset af den eventuelle udvikling, vil de samle alle relevante parter i en konference på højt plan og vurdere fremskridtene i løbet af 12 måneder.

[32] Strategien vil blive finansieret inden for rammerne af de beløb, der er forudset for hvert af de relevante politikområder (CEF, Horisont 2020, Fonden for Intern Sikkerhed, FUSP og eksternt samarbejde, navnlig stabilitetsinstrumentet) som fastsat i Kommissionens forslag om den flerårige finansielle ramme 2014-2020 (med forbehold af budgetmyndighedens godkendelse og de endelige beløb i den vedtagne FFR for 2014-2020). Hvad angår behovet for at sikre overordnet sammenhæng med antallet af disponible stillinger til decentrale organer og underloftet for decentrale organer under de enkelte udgiftsområder i den næste FFR, vil de organer (Cepol, EDA, ENISA, Eurojust og Europol/EC3), der i denne meddelelse anmodes om at påtage sig nye opgaver, blive tilskyndet til at sørge herfor, for så vidt som det er fastslået, at organet rent faktisk har kapacitet til at absorbere øgede ressourcer, og alle muligheder for omfordeling er klarlagt.